Highly Reliable Intrusion Detection Model as a Predictive Framework for Network Data Traffic Analysis in Wireless Networks

Reshma Ashik Chauhan

Senior Research Analyst, SMRVD Security Solutions, India.

Abstract: It has become an important model in various applications such as education, business and others. So security of the data that is communicated through internet is necessary. Secure network is maintained by Intrusion Detection System (IDS). IDS observes the data traffic carefully and identifies it as normal or spam. Nowadays most of the applications depends on the advance network technologies namely wireless networks, wireless sensor networks and Bluetooth. In case of wireless sensor networks security mechanisms such as key-management protocols, authentication techniques and security protocols cannot be used because of resource constraints. Intrusion Detection System is the ideal security mechanism for wireless sensor networks. In this paper classification and predictive models for intrusion detection are built by using machine learning classification algorithms.

Keywords: Threat Analysis; Information Security; Data security.

1. Introduction

A security mechanism used to monitor the abnormal behavior of the network is an Intrusion Detection System (IDS). The IDS identifies and informs that whether the user activity is normal or not. The user's activities are compared by the IDS with the already stored intrusion records to identify the intrusion.

Accurate predictive models can be built for large data sets using supervised machine learning techniques that are not possible by traditional methods [1-7]. As specified by Tom Mitchell, machine learning based intrusion detection falls under two categories Anomaly and Misuse. IDS learns the patterns by the training data, so the misuse based method is used. Misuse based detection can detect only the known attack, new attacks cannot be identified. Anomaly based IDS observes the normal behavior and if there is a change in the behavior then it considers that behavior as anomaly. So anomaly based IDS can detect new attacks that are not learned from the training model.

Till now different machine learning techniques such as artificial neural networks, Support Vector Machine and Naive Bayes based techniques are proposed for the intrusion detection. A new detection by combining different techniques, a hybrid detection technique is proposed. The literature on comparison of supervised machine learning techniques in intrusion detection is limited [8-19]. Hence this paper aims at understanding the implications of using supervised machine learning techniques on intrusion detection.

Recently authors used algorithms namely Random Forest, Naive Bayes, K-means and Support Vector Machine to identify four types of attacks. They also proposed best feature selection method. Concluded that the Random Forest Classifier (RFC) outperforms the other methods. They have mentioned that hierarchical clustering method can be used to improve the performance.

Authors proposed semi supervised machine learning based intrusion detection. Authors have not considered the resource consumption. Combination of different classifiers to identify the intrusion is proposed. They used supervised classification or unsupervised clustering for filtering of the data. They used NSL-KDD data-set and tested with decision tree classifier [20-29]. But the proposed method works only for binary class classification. Authors proposed intrusion detection system using supervised machine learning techniques to identify the on line network data as normal or not. The proposed method identifies probe and Denial of Service attacks only, but the other attacks are not considered.

A framework of machine learning approach is proposed. Intrusion is identified by analyzing the local features. Researchers proposed Naive Bayes based multiclass classifier to identify the intrusions. They suggested that intrusion detection is possible by Hidden Naive Bayes (HNB) model.

Denial of Service attacks is identified with good accuracy compared to other attacks. Studies suggested Intrusion detection technique using Support Vector Machine (SVM). They also used feature removal method to improve the efficiency. Using the proposed feature removal method they selected best nineteen features from the KDD-CUP99 data-set. In the proposed method the data set used is very small [30-43]. A light weight IDS is proposed. The proposed method mainly focused on pre-processing of the data so that only important attributes can be used. The first step is to remove the redundant data so that the learning algorithms give the unbiased result.

A survey on intrusion detection systems was conducted. Information about IDSs such as classification, Intrusion type, computing location and infrastructure are discussed. They discussed about the Mobile Adhoc Networks (MANET) IDS. They compared MANETIDS and the Wireless Sensor Networks (WSN) IDS. Authors suggested that for mobile applications distributed and cooperative IDS schemes are suitable. For stationary applications centralized IDSs are suitable and for cluster based applications hierarchical IDSs are suitable. Authors proposed intrusion detection framework to detect routing attacks.

Specification based approach is used to detect routing attacks. Authors claim that the proposed method has low False Positive Rate (FPR) and good intrusion detection rate. The proposed method works only for static networks [44-56]. Investigators developed IDS for Sink, Cluster Head (CH) and for a Sensor Node (SN) separately and combined altogether to identify the intrusion in heterogeneous Cluster Based Wireless Sensor Networks (CWSN) but the detection rate for U2R, R2L and Probe attacks is very low.

2. Machine LearningTechniques

This work is to design a network intrusion detection system with the different supervised machine learning classifiers. This paper is to investigate the performance of the classifiers namely Logistic Regression, Support Vector Machine (SVM), Gaussian Naive Bayes (GNB) and Random Forest in intrusion detection. These classifiers are discussed below.

Logistic regression - To solve the classification problems Logistic Regression (LR) is used. TLR works for both binary classification and multiclass classification. Probability of occurrence of an event is predicted by fitting data to the Logistic function. The values selected by the logistic function are in the range 0 and 1. If the value is 0.5 and above then it is labeled as otherwise 0.

Support vector machine - Mainly for classification problems Support Vector Machine algorithm is used, but it can be used in regression problems also. N-dimensional feature space is considered to plot each data item as a point with the value of each feature as a particular coordinate. Then classification is made by finding the hyper-plane that differentiates the two classes very well. Support Vectors are the co-ordinates of specific observation that lies closest to the boarder line. In case of SVM training samples are divided into different subsets called as support vectors, the decision function is specified by these support vectors. This paper is based on the liner kernel method of SVM for intrusion detection.

Gaussian naive Bayes - The Gaussian Naive Bayes algorithm is the supervised learning method. Probabilities of each attribute whichbelongs to each class are considered for a prediction. This algorithm is assumes that the probability of each attribute belonging to a given class value is not depends on all other attributes. If the value of the attribute is known the probability of a class value is called as the conditional probabilities. Data instances provability can be found out by multiplying all attributes conditional probabilities together. Prediction can be made by calculating the each class instanceprobabilities and by selecting the highest probability class value.

Random forest classifier - In 2001 Breiman proposed the random forest machine learning classifier. It is a collaborative method which works based on the proximity search. It is decision tree based classifier. It makes use of standard divide and conquers approach to improve the performance. The main principle behind random forest is that strong learner group is created by a group of weak learners. It is applicable to disjunctive hypothesis.

2.1. Intrusion Detection

The standard intrusion detection data set KDDCUP9923 has redundant records. This may lead to unfair result of the machine learning algorithms. So the supervised machine learning algorithms are tested NSL-KDD24 data-set which is the advanced version of the KDDCUP99 intrusion detection data-set. It has 42 features and the four simulated attacks. Denial of Service (DoS) attack: Over usage of the bandwidth or non-availability of the system resources leads to the DoS attacks. Examples: Neptune, Teardrop and Smurf.

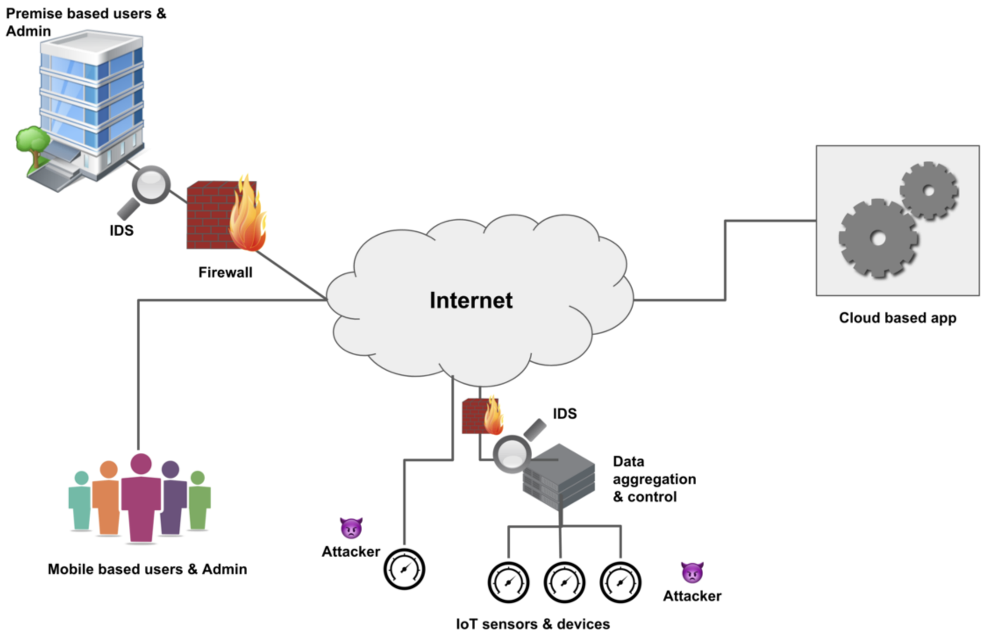
Premise based users & Admin
IDS
Firewall
Internet
Cloud based app
IDS
Data aggregation & control
Mobile based users & Admin
Attacker
Attacker
IoT sensors & devices

Fig.1. Existing Methodology (Source: Internet)

User to Root (U2R) Attack: Initially attacker access normal user account, later gain access to the root by exploiting the vulnerabilities of the system. Examples: Perl, Load

Module and Eject attacks. Probe Attack: Have an access to entire network information before introducing an attack. Examples: ipsweep, nmap attacks. Root to Local (R2L) Attack: By exploiting some of the vulnerabilities of the network attacker gains local access by sending packets on a remotemachine. Examples: imap, guess password and ftp- write attacks.

In pre- processing step all the categorical data which are in textual form are converted to numerical form. Pre-processed data is divided as testing data and training data. The models are built using Logistic Regression, Gaussian Naive Bayes, Support Vector Machine and Random Forest classifiers. These models are used for predicting the labels of the test data. Actual labels and predicted labels are compared. Accuracy, True Positive Rate (TPR) and False Positive Rate (FPR) are computed. Based on these parameters performance of the models are compared. Following steps are used to build the models.

- Pre-process the data set.
- The data set is divided as training data and testing data
- Build the classifier model on training data for
- Logistic Regression
- Support Vector Machine
- Gaussian Naive Bayes
- Random Forest
- Read the test data
- Test the classifier models on training data
- Compute and compare TPR, FPR, Precision, Recall, F1-Score and Accuracy for all the models.

Supervised machine learning algorithms namely Logistic Regression, Gaussian Naive Bayes, Support Vector Machine and Random Forest are tested on NSL-KDD dataset, the new standard intrusion detection data-set. These algorithms are tested on Intel Core (TM) i5-3230M CPU @2.60 GHZ, 4 GB RAM and coding is done by Python. The result of the experiment is represented as a Reliability curve. In Reliability curve estimated probabilities are plotted against the true empirical probabilities. The Reliability Curve for the above mentioned supervised machine learning classifiers. Reliability curve for the ideal classifier falls near the diagonal because the estimated probabilities and empirical probabilities are nearly equal.

Estimated probabilities values ranging from 0 to 0.1, to 0.2 and so on. The values 0 to 0.1 belongs to I bin, 0.1 to 0.2 belongs to II bin and similarly the other ranges. It can be concluded that theRandom Forest classifier out performs the other methods in identifying the network traffic as normal or an attack. Whereas the SVM identifies the intrusion with the lowest probability estimate.

Quality of the classification models is identified by plotting the Receiver Operating Characteristics (ROC) curve. Random Forest has highest TPR. Hence, the ROC curve for Random forest is plotted separately. By observing the graphs, it can be concluded that the Random forest classifier has lowest FPR and highest TPR in identifying attacks. It outperforms the other techniques. Whereas Support Vector Machine has highest FPR (39%) and minimal TPR (75%) for intrusion detection.

This is due to the fact that too many features from the data set is considered15 and SVM's linear kernel function is used. Based on the results it can be identified that Random Forest classifier with the highest accuracy, outperforms the other methods. Whereas SVM has the lowest accuracy, Logistic Regression algorithm has the good accuracy than Gaussian Naive Bayes and SVM.

3. Conclusions

With the rapid development of real-time big data and the Internet of Things, the demand for surrounding environmental data has also increased significantly. The demand for WSN products with low node costs and easy deployment will gradually expand. WSN products can break through traditional detection methods. They reduce the costs of environmental testing, and also greatly reduce the cumbersome process of traditional testing methods. As a new network, the WSN has been widely studied by scientific researchers and widely used in industry since its inception. Common applications include scenarios such as environmental detection, military operations, and information positioning. An attempt has been made to check the performance of the supervised machine learning classifiers namely Support Vector Machine, Random Forest, Logistic Regression and Gaussian Naive Bayes are compared for intrusion detection.

References

[1] B. Halak, M. Zwolinski, M. S. Mispan, "Overview of PUF-based hardware security solutions for the internet of things," in Proceedings of 2016 IEEE 59th International Midwest

Symposium on Circuits and Systems (MWSCAS), Abu Dhabi, United Arab Emirates, 2016;pp. 1-4.

[2] D. M. Mendez, I. Papapanagiotou, and B. Yang, 2017 (Online). Available:, https://arxiv.org/abs/1707.01879

[3] D. Shreenivas, S. Raza, T. Voigt, "Intrusion detection in the RPL-connected 6LoWPAN networks," in Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi, United Arab Emirates, 2017;pp. 31-38.

[4] Vinod Varma Vegesna (2018). “Analysis of Artificial Intelligence Techniques for Network Intrusion Detection and Intrusion Prevention for Enhanced User Privacy”, Asian Journal of Applied Science and Technology, Volume 2, Issue 4, Pages 315-330, Oct-Dec 2018, Available at SSRN: https://ssrn.com/abstract=4418114

[5] Vinod Varma Vegesna (2017). “Incorporating Wireless Sensor Networks and the Internet of Things: A Hierarchical and Security-Based Analysis,” International Journal of Current Engineering and Scientific Research, Volume-4, Issue-5, Pages 94-106, Available at SSRN: https://ssrn.com/abstract=4418110

[6] Hamid Ali Abed Al-Asadi and et al., “Priority Incorporated Zone Based Distributed Clustering Algorithm For Heterogeneous Wireless Sensor Network”, Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 5, PP. 306-313, 2019.

[7] Hamid Ali Abed Al-Asadi and et al., “A Network Analysis for Finding the Shortest Path in Hospital Information System with GIS and GPS, Journal of Network Computing and Applications (2020) 5: 10-22.

[8] Vinod Varma Vegesna (2016). “Threat and Risk Assessment Techniques and Mitigation Approaches for Enhancing Security in Automotive Domain,” International Journal of Management, Technology And Engineering, Volume VI, Issue II, July-Dec 2016, Pages 314-331, Available at SSRN: https://ssrn.com/abstract=4418100

[9] Vinod Varma Vegesna (2015). “Incorporating Data Mining Approaches and Knowledge Discovery Process to Cloud Computing for Maximizing Security,” International Journal of Current Engineering and Scientific Research, Volume-2, Issue-6, Pages 118-133, Available at SSRN: https://ssrn.com/abstract=4418107

[10] S. Fosso Wamba, A. Anand, L. Carter, "A literature review of RFID-enabled healthcare applications and issues," International Journal of Information Management, vol. 33, no. 5, pp. 875-891, 2013.

[11] T. Jiang, G. Wang, H. Yu, "A dynamic intrusion detection scheme for cluster-based wireless sensor networks," in World Automation Congress 2012Puerto V allarta, Mexico, pp.

259-261, 2012.

[12] T. Sherasiya, H. Upadhyay, H. B. Patel, "A survey: intrusion detection system for Internet of Things," International Journal of Computer Science and Engineering, vol. 5, no. 2, pp. 91-98, 2016.

[13] E. Benkhelifa, T. Welsh, W. Hamouda, "A critical review of practices and challenges in intrusion detection systems for IoT: toward universal and resilient systems," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3496-3509, 2018.

[14] G. Han, J. Jiang, W. Shen, L. Shu, J. Rodrigues, "IDSEP: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks," IET Information Security, vol. 7, no. 2, pp. 97-105, 2013.

[15] Vinod Varma Vegesna (2021). “The Utilization of Information Systems for Supply Chain Management for Multicomponent Productivity Based on Cloud Computing,” International Journal of Management, Technology and Engineering, Volume XI, Issue IX, September 2021, Pages 98-113.

[16] Vinod Varma Vegesna (2021). “The Applicability of Various Cyber Security Services for the Prevention of Attacks on Smart Homes,” International Journal of Current Engineering and Scientific Research, Volume-8, Issue-12, Pages 14-21.

[17] Hamid Ali Abed Al-Asadi, et al., “Nature Inspired Algorithms multi-objective histogram equalization for Grey image enhancement”, Advances in Computer, Signals and Systems (2020) 4: 36-46 Clausius Scientific Press, Canada DOI: 10.23977/acss.2020.040106.

[18] Hamid Ali Abed Al-Asadi and et al., “ Critical Comparative Review of Nature-Inspired Optimization Algorithms (NIOAs), International Journal of Simulation: Systems, Science and Technology (IJSSST), 2020, 21(3), PP1-15

[19] Hamid Ali Abed Al-Asadi, (2022) “1st Edition: Privacy and Security Challenges in Cloud Computing A Holistic Approach" Intelligent Internet of Things for Smart Healthcare Systems, Scopus, Taylor @Francis, CRC Press. (Book Chapter: Enhanced Hybrid and Highly Secure Cryptosystem for Mitigating Security Issues in Cloud Environments), March 2022.

[20] Vinod Varma Vegesna (2020). “Secure and Privacy-Based Data Sharing Approaches in Cloud Computing for Healthcare Applications,” Mediterranean Journal of Basic and Applied Sciences, Volume 4, Issue 4, Pages 194-209, October-December 2020, doi: 10.46382/mjbas.2020.4409.

[21] Vinod Varma Vegesna (2019). “Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes”, Indo-Iranian Journal of Scientific Research, Volume 3, Issue 1, Pages 69-84, January-March 2019, Available at

SSRN: https://ssrn.com/abstract=4418119

[22] M. S. V an Devender, W. B. Glisson, M. Campbell, M. A. Finan, "Identifying opportunities to compromise medical environments," in Proceedings of Twenty-second Americas Conference on Information Systems, San Diego, CA, 2016;pp. 1-9.

[23] N. K. Thanigaivelan, E. Nigussie, R. K. Kanth, S. Virtanen, J. Isoaho, "Distributed internal anomaly detection system for Internet-of-Things," in Proceedings of 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las V egas, NV, 2016;pp. 319-320.

[24] P. Kasinathan, C. Pastrone, M. A. Spirito, M. Vinkovits, "Denial-of-service detection in 6LoWP AN based Internet of Things," in Proceedings of 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, 2013;pp. 600-607.

[25] Vinod Varma Vegesna (2022). “Accelerate the development of a business without losing privacy with the help of API Security Best Practises - Enabling businesses to create more dynamic applications,” International Journal of Management, Technology and Engineering, Volume XII, Issue IX, September 2022, Pages 91-99.

[26] Vinod Varma Vegesna (2022). “Investigations on Cybersecurity Challenges and Mitigation Strategies in Intelligent transport systems,” Irish Interdisciplinary Journal of Science and Research, Vol. 6, Iss. 4, Pages 70-86, October-December 2022, doi: 10.46759/iijsr.2022.6409.

[27] Hamzah F. Zmezm, Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, "A Novel Scan2Pass Architecture for Enhancing Security towards E-Commerce," Future Technologies Conference 2017, 29-30 November 2017 | Vancouver, BC, Canada, 2017.

[28] Hamid Ali Abed Al-Asadi, Majida Ali Al-Asadi, Nada Ali Noori , "Optimization Noise Figure of Fiber Raman Amplifier based on Bat Algorithm in Optical Communication network," International Journal of Engineering & Technology, Scopus, Vol 7, No 2, pp. 874-879, 2018.

[29] Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, Hamzah F. Zmezm, Dr. Hussain Falih Mahdi, Hassan Muhsen Abdulkareem Al-Haidari. "Suggested Mechanisms for Understanding the Ideas in Authentication System," International Journal of Advancements in Computing Technology9(3):10-24, 2018.

[30] Vinod Varma Vegesna (2021). “Analysis of Data Confidentiality Methods in Cloud Computing for Attaining Enhanced Security in Cloud Storage,” Middle East Journal of Applied Science & Technology, Vol. 4, Iss. 2, Pages 163-178, April-June 2021, Available at

SSRN: https://ssrn.com/abstract=4418127

[31] Vinod Varma Vegesna (2021). “A Highly Efficient and Secure Procedure for Protecting Privacy in Cloud Data Storage Environments,” International Journal of Management, Technology and Engineering, Volume XI, Issue VII, July 2021, Pages 277-287.

[32] L. Buczak, E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, 2016.

[33] Milenkoski, M. Vieira, S. Kounev, A. Avritzer, B. D. Payne, "Evaluating computer intrusion detection systems: a survey of common practices," ACM Computing SurveysArticle no.12, vol. 48, no. Article 12, 2015.

[34] B. Zarpelao, R. S. Miani, C. T. Kawakani, S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," Journal of Network and Computer Applications, vol. 84, pp. 25-37, 2017.

[35] G. Padmavathi, D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," International Journal of Computer Science and Information Security, vol. 4, no. 1 & 2, pp. 1-9, 2009.

[36] Vinod Varma Vegesna (2023). “A Comprehensive Investigation of Privacy Concerns in the Context of Cloud Computing Using Self-Service Paradigms,” International Journal of Management, Technology and Engineering, Volume XIII, Issue VII, July 2023, Pages 173-187.

[37] Vinod Varma Vegesna (2022). “Using Distributed Ledger Based Blockchain Technological Advances to Address IoT Safety and Confidentiality Issues,” International Journal of Current Engineering and Scientific Research, Volume-9, Issue-3, Pages 89-98.

[38] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "Simplifying Handwritten Characters Recognition Using a Particle Swarm Optimization Approach”, European Academic Research, Vol 1,pp. 535- 552, Issue(5), 5. 2013.

[39] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "High Accuracy Arabic Handwritten Characters Recognition using (EBPANN) Architecture," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6 Issue 2, 2015.

[40] Hamid Ali Abed Al-Asadi and Majda Ali Abed, "Object Recognition Using Artificial Fish Swarm Algorithm on Fourier Descriptors," American Journal of Engineering, Technology and Society; Volume 2, Issue 5: pp. 105-110, 2015.

[41] Vinod Varma Vegesna (2022). “Methodologies for Enhancing Data Integrity and Security in Distributed Cloud Computing with Techniques to Implement Security Solutions,”

Asian Journal of Applied Science and Technology, Volume 6, Issue 2, Pages 167-180, April-June 2022, doi: 10.38177/ajast.2022.6217.

[42] Vinod Varma Vegesna (2022). “Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks,” International Journal of Management, Technology and Engineering, Volume XII, Issue VII, July 2022, Pages 81-94.

[43] K. Xing, F. Liu, X. Cheng, D. H. C. Du, "Real-time detection of clone attacks in wireless sensor networks," in Proceedings of 2008 The 28th International Conference on Distributed Computing Systems, Beijing, China, 2008;pp. 3-10.

[44] M. Nawir, A. Amir, N. Yaakob, O. B. Lynn, "Internet of Things (IoT): taxonomy of security attacks," in Proceedings of 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, 2016;pp. 321-326.

[45] Vinod Varma Vegesna (2023). “Adopting a Conceptual Architecture to Mitigate an IoT Zero-Day Threat that Might Result in a Zero-Day Attack with Regard to Operational Costs and Communication Overheads,” International Journal of Current Engineering and Scientific Research, Volume-10, Issue-1, Pages 9-17.

[46] Vinod Varma Vegesna (2023). “Methodology for Mitigating the Security Issues and Challenges in the Internet of Things (IoT) Framework for Enhanced Security,” Asian Journal of Basic Science & Research, Vol. 5, No. 1, January-March 2023, Pages 85–102, doi: 10.38177/ajbsr.2023.5110.

[47] Hamid Ali Abed Al-Asadi, Majida Ali Abed, AL-Asadi, Zainab sabah, Baha Al-Deen, Ahmad Naser Ismail, “Fuzzy Logic approach to Recognition of Isolated Arabic Characters”, International Journal of Computer Theory and Engineering, Vol. 2, No. 1, 1793-8201, February, 2010.

[48] H. A. Al-Asadi, M.H. Al-Mansoori, S. Hitam, M. I. Saripan, and M. A. Mahdi, “Particle swarm optimization on threshold exponential gain of stimulated Brillouin scattering in single mode fibers,” Optics Express, vol. 19, no. 3, pp. 1842-1853, 2011.

[49] Majida Al-Asadi, Yousif A. Al-Asadi, Hamid Ali Abed Al-Asadi, "Architectural Analysis of Multi-Agents Educational Model in Web-Learning Environments," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 6, 2012.

[50] Vinod Varma Vegesna (2023). “Secure and Reliable Designs for Intrusion Detection Methods Developed Utilizing Artificial Intelligence Approaches,” International Journal of Current Engineering and Scientific Research, Volume-10, Issue-3, Pages 1-7.

[51] Vinod Varma Vegesna (2023). “A Critical Investigation and Analysis of Strategic

Techniques Before Approving Cloud Computing Service Frameworks," International Journal of Management, Technology and Engineering, Volume XIII, Issue IV, April 2023, Pages 132-144.

[52] Alqassem, D. Svetinovic, "A taxonomy of security and privacy requirements for the Internet of Things (IoT)," in Proceedings of 2014 IEEE International Conference on Industrial Engineering and Engineering Management, Bandar Sunway, Malaysia, 2014;pp. 1244-1248.

[53] J. Deogirikar, A. Vidhate, "Security attacks in IoT: a survey," in Proceedings of 2017 International Conference on I-SMAC (IoT Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017;pp. 32-37.

[54] P. Sethi, S. R. Sarangi, "Internet of Things: architectures, protocols, and applications," Journal of Electrical and Computer Engineering, vol. 2017, no. 9324035, 2017.

[55] R. P. Kurbah, B. Sharma, "Survey on issues in wireless sensor networks: attacks and countermeasures," International Journal of Computer Science and Information Security, vol. 14, no. 4, pp. 262-269, 2016.

[56] H. A. Abdul-Ghani, D. Konstantas, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: an IoT perspective," Journal of Sensor and Actuator Networks pp. 22, vol. 8, no. 2, 2019.